Office of Information Security
OCIO

Disaster Recovery Coordinators' Meeting

January 20, 2010

Meeting Agenda

Office of Information Security
OCIO

- Short Subjects
  - SIMM Form Changes and Annual Filing Reminder
  - Leader List Updates
  - Enterprise Risk Assessment Grant
- CA Information Security Strategic Plan
- New Information Security/Disaster Recovery Policy
  - Policy, Standards, Procedures, Guidelines
  - Phase I, Vetting Complete
  - Phase II, Preparing to Vet
  - Phase III, Vetting in March (includes DR Policy)
  - Phase IV, TBD

Meeting Agenda

Office of Information Security
OCIO

Security and Capacity

- Draft Telework IT Policy Letter and Standard

Upcoming Opportunities

- CISO Lecture Series, February 25, 2010, DGS
- Golden Guardian 2011, Flood Scenario
- New CalEMA Continuity Planning Guidance and Plan Template
- Free FEMA/DHS Training
  - MTG 331-1 Implementing Continuity of Operations Planning Course
  - Homeland Security Exercise and Evaluation Program (HSEEP) Course

SIMM Form Changes and Annual Filing Reminder

- Name Change from OISPP to OIS
- Other minor clarification changes
- SIMM70A (Agency Designation Letter)
- SIMM70C (Agency Risk Management and Privacy Program Compliance Certification)
- Forms due February 1, 2010

http://www.cio.ca.gov/OIS/Government/activities_schedule.asp

Leader List Updates

- Information Security Officers
- Privacy Officers and
- DR Coordinators
- All available on website updated 11/30/09
- http://www.cio.ca.gov/OIS/Government/events/default.asp#SMeetings

State Enterprise Cyber Security Risk Program – Grant B

- Nineteen (19) month project with specific deliverables.
- … leverage NIST 800-30, modified to meet California's needs, as a standard to better identify and manage risks across the enterprise …
- The risk assessment process will integrate a series of interviews, system level vulnerability assessments, documentation reviews and analysis to identify known risks and measure the effectiveness of current controls to mitigate known risks.
- Includes funding for hardware, software, training, and consulting.

California Information Security Strategic Plan

Office of Information Security
OCIO

California Information Security Strategic Plan

October

2009

Cybersecurity and Privacy Concepts, Strategies & Goals
Volume 4

Arnold Schwarzenegge
Governo

Teri Taka
Chief Information Officer, Office of the CI

Mark Weatherfor
Chief Information Security Officer, Office of Information Securit

OCIO 2009 Information Technology Strategic Plan

Six Strategic Concepts

- IT as reliable as electricity
- Fulfilling technology's potential to transform lives
- Self-governance in the digital age
- Information as an asset
- Economic and sustainable
- Facilitating collaboration that breeds better solutions

Weblink:
http://www.cio.ca.gov/OIS/Government/documents/pdf/California_Information_Security_Strategic_Plan_2009.pdf

Information Security Policy Phase I – Vetting Complete

- 5300 Information Security Policy
- 5305 Risk Management
- 5305-P1 Risk Assessment Procedure
- 5310 Policy Management

Information Security Policy
Phase II – Preparing to Vet

5315	Organization
5320.1	Information Asset Oversight
5320.2	Information Asset Trustees
5320.3	Users of Information Assets
5320-S1	Information Asset Classification Standard
5320-S2	Information Asset Handling Standard
5330.1	Facility Leader Responsibilities
5330.2	Information Asset Trustee Responsibilities
5340.1	Access Management Standard
5340.2	User Responsibilities
5340-S1	User Access Management Standard
5340-S2	Password Management Standard

Office of Information Security
OCIO

Information Security Policy

Phase III – Vetting March 2010;
Includes DR Policy/Standards

Phase IV -- TBD

Telework ITPL and Standard

[excerpt from draft; **available for review until 1/21/2010**]
http://www.cio.ca.gov/wiki/Policy%20and%20Standards%20Review.ashx

PURPOSE:

The purpose of this Information Technology Policy Letter (ITPL) is to establish the Telework Security Standards in the Statewide Information Management Manual (SIMM) Section 85B as requirements for state government agencies and departments.

POLICY:

Agency heads shall ensure that only authorized users who have been trained regarding their roles and responsibilities, security risks, and the requirements included in the referenced standards, be permitted to telework.

Telework ITPL and Standard

[excerpt from draft]

Office of Information Security
OCIO

State Information Management Manual Section 85 B.

- … agency heads shall ensure that managers, supervisors, and telework users receive security training ..
- Only authorize telework user access to resources which are necessary to carry out the telework arrangement safely and securely. … Telework user accounts shall, as a rule, be set up to have limited privileges.
- Telework user accounts shall require two-factor authentication, except when using a Web-based connection, such as Outlook Web Access (OWA) or other similar interface.

Telework ITPL and Standard

[excerpt from draft]

Office of Information Security
OCIO

State Information Management Manual Section 85 B.
(continued)

- Agency IT Administrators shall log and monitor all telework access. Log files shall capture sufficient detail to allow a virtual reconstruction of the end-to-end network session.
- Telework users shall not connect personally-owned information assets to the state IT infrastructure at the network-level unless an approved written exception applies and is implemented in accordance with the additional standards which apply to use of personally-owned information assets herein.

CISO Lecture Series

Office of Information Security
OCIO

SAVE THE DATE! You won't want to miss this event.

The next CISO Lecture Series will be a special **full-day** event to be held on **February 25, 2010** at the **Department of General Services' Auditorium (Ziggurat Building), 707 Third Street, West Sacramento, CA 95605-2811**. Parking is available in the parking garage located on the north side of the Ziggurat Building, available from 6:00 a.m. to 6:00 p.m. at a cost of $1.00 per half an hour up to a maximum of $12.00 per day. There is also limited street parking (90 minute and 2 hour). For directions to the Ziggurat Building, visit http://www.dgs.ca.gov/ContactUs/ZigDir.htm.

We have several dynamic speakers giving presentations on some relevant topics including:

Mr. John Streufert, CISO, U.S. State Department
Mr. Randy Vickers, Director, United States Computer Emergency Readiness Team (US-CERT)
Mr. Patrick Beggs, Director, Cyber Security Evaluations at Department of Homeland Security/National Cyber Security Division (DHS/NCSD)
Mr. Larry Rohrbough, Executive Director, TRUST Science & Technology Center, University of California, Berkeley

Event and registration details will be coming soon.

Upcoming Opportunities

☑ **Golden Guardian 2011** – Flood Scenario
Concept and Objectives Conference
January 28, 2010

☑ **New Continuity Planning Guidance** and
Plan Template: **Preparing the State**
(**Link** on CalEMA or OES websites on *lower left*;
Continuity of Government Operations)
http://www.oes.ca.gov/WebPage/oeswebsite.nsf/Content/E5EB6F0DF18C155C8825740C0081FD9F?OpenDocument

☑ Free FEMA/DHS Training:

http://www.ohs.ca.gov/pdf/January_2010_Training_Bulletin.pdf
View monthly training bulletin; watch for Sacramento offerings for:

- **MGT 331-1 Implementing Continuity of Operations Planning Course**
- **Homeland Security Exercise and Evaluation Program (HSEEP) Course (April 5-8, 2010)**

OR CALL:
Ramon Barboa at 916-322-2988 or email:
ramon.barboa@ohs.ca.gov

Office of Information Security
OCIO

Questions